https://www.forbes.com/sites/forbestechcouncil/2019/01/15/2019-data-privacy-wish-list-moving-from-compliance-to-concern/#43f9caae2493

Jan 15, 2019, 08:45am

2019 Data Privacy Wish List: Moving From Compliance To Concern

Ameesh Divatia Forbes Councils
Forbes Technology Council CommunityVoice

Post written by Ameesh Divatia

Ameesh Divatia is Co-Founder and CEO of Baffle, Inc., with a proven track record of turning innovative ideas into successful businesses.

For virtually every business, the last and first (calendar) quarters are filled with reflection and planning — for revenue, services, operations, budgeting and, of course, privacy and security. Throughout the year, I've spent a lot of time in my column examining emerging trends, both slow and rapid, in data privacy and security. As you're completing those spreadsheets and presentations, including the annual budgetary ask, I thought it would be useful to build upon those insights and look at what to prepare for this year.

Data Privacy And Protection Laws

The General Data Protection Regulation is now in full effect to protect the privacy of European Union citizens. The California Consumer Privacy Act passed in June 2018 and goes into effect in January 2020. New York has cybersecurity regulations specifically for financial institutions. Work in Brazil? It has passed one as well. It's a messy landslide of different laws that can keep your legal and compliance teams running in circles.

Don't get me wrong: increased privacy protection laws are good and badly needed. However, virtually borderless internet and cloud initiatives make legal lines harder to identify, correlate and combine. Also, privacy regulations are not specifying how the data is to be protected. All they say is that if cleartext data is lost, it is mandatory to notify the affected parties and the regulators about that breach. Organizations can easily find themselves ping-ponging between compliance rules, and as I've said in the past, just checking compliance boxes has proven time and time again to be a failed security — and now privacy — strategy.

A Move From Privacy 'Compliance' to 'Concern and Care'

Organizations need to significantly shift their mindset about data privacy. I've argued that it starts with the appointment of a data protection officer and then goes from a compliance mindset and approach to one of data protection and stewardship. Companies argue that they need the data and they need to gather it aggressively in order to determine its value with analytics. However, this approach presents a Catch-22. The popular argument that we should be more careful with customer data is the new oil of the 21st century. It's not just about compliance anymore, but rather a philosophy that treats data with extreme care and with prevention of data breaches in mind.

Amplify Automation And Monitoring

Despite the advances (or hype, but that's for another column) in artificial intelligence and machine learning, humans still run businesses. Even with the best intentions, human beings make mistakes, which helps explain why phishing still remains such an effective tactic. They may go into a project with all the care in the world, but they still leave doors unlocked and create any number of errors that expose data.

Technology researchers at Gartner, Inc. have noted that security detection and response — rather than just preventative measures — is a now a top priority for enterprises. With a worldwide shortage of nearly one million security professionals, we must automate routine processes amplify the impact of trained humans. Gartner predicts that by 2021, automation will be heavily weighted by one-fifth of all security buyers.

Reexamine Third-Party Partners And Their Data Access

Corporate walls have become increasingly transparent, and are not just confined to your full-time employees. Two years ago, half -- yes, half -- of all organizations experienced a data breach because of a business vendor or associate. While this may be getting better thanks to new privacy legislation and advances in encryption and other security solutions, the percentage of breaches still remains high.

In healthcare — a business ecosystem entrenched in a complicated mesh of third-party providers — there's some action underway. In August 2018, CISOs at some of the largest health providers formed a consortium to help address third-party risk. Other industries should also find a common set of strict data care policies and technologies that must be followed, rather than operating on a case-by-case or contract-by-contract basis.

But there's no need to wait for a consortium or a compliance standard to do the right thing with privacy and security of data. Your customers demand better care of their data. Use your 2019 planning to establish best practice guidelines for your organization, and then share those policies (and lessons learned) with your industry peers. But most importantly, shift your mindset to one of extreme concern and care for customer information and privacy — not just regulatory compliance.

Forbes Technology Council is an invitation-only community for world-class CIOs, CTOs and technology executives. ***Do I qualify?***

Ameesh Divatia Forbes Councils

Ameesh Divatia is Co-Founder & CEO of Baffle, Inc., with a proven track record of turning innovative ideas into successful businesses.

Forbes Technology Council CommunityVoice

Forbes Technology Council is an invitation-only, fee-based organization comprised of leading CIOs, CTOs and technology executives. Find out if you qualify at forbestechcouncil.com. Questions about an article? Email feedback@forbescouncils.com.